**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | |
|---|---|
| U.S. PATENT APPLICATION NUMBER | 10/683,564 |
| FILING DATE | 10 October 2003 |
| INVENTOR | Keith Woodard et al. |
| ASSIGNEE | Symantec Corporation |
| GROUP ART UNIT | 2141 |
| EXAMINER | Djenane M. Bayard |
| TITLE | METHOD AND SYSTEM FOR SCANNING NETWORK DEVICES |
| ATTORNEY'S DOCKET NO. | 55994.0136 |

**APPEAL BRIEF**

To: MS Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

From: Bryan K. Hanks
HOLLAND & HART LLP
P.O. Box 11583
Salt Lake City, UT 84147-0583
Telephone: (801) 799-5800
Facsimile: (801) 799-5700

Dear Sir:

In accordance with 37 C.F.R. § 41.37(a), Appellants respectfully submit this Appeal Brief in furtherance of the Notice of Appeal filed in the above-identified application on 23 May 2008, which appeals the final Office Action dated 3 March 2008 ("final Office Action").

This Appeal Brief contains items under the following headings, as required by 37 C.F.R. § 41.37 and MPEP 1205:

I. Real Party In Interest

II. Related Appeals and Interferences

III. Status of Claims

IV. Status of Amendments

V. Summary of Claimed Subject Matter

VI. Grounds of Rejection to be Reviewed on Appeal

VII. Arguments

VIII. Claims Appendix

IX. Evidence Appendix

X. Related Proceedings Appendix

XI. Conclusion

The fees required under 37 C.F.R. § 41.20(b)(2) are provided in the accompanying TRANSMITTAL OF APPEAL BRIEF. In compliance with 37 C.F.R. § 41.37(a)(1), Appellants submit one (1) copy of this Appeal Brief.

## I. REAL PARTY IN INTEREST

Symantec is the real party in interest in the present application. An assignment of all rights in the present application to Symantec Corporation was recorded by the U.S. Patent and Trademark Office on 6 September 2007 at Reel 019790, Frame 0082.

## II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

Appellants are not aware of any other appeals, interferences, or judicial proceedings that will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

## III. STATUS OF CLAIMS

### *A. Total Number of Claims in Application*

There are 43 claims currently pending in the present application: claims 1-10, 12-25, 27-34, and 36-46.

### *B. Current Status of Claims*

1. Objected-to claims: None
2. Cancelled claims: claims 11, 26, and 35
3. Claims withdrawn from consideration but not canceled: None
4. Allowed claims: None
5. Rejected claims: 1-10, 12-25, 27-34, and 36-46.

### *C. Claims On Appeal*

Appellants are appealing the rejection of claims 1-10, 12-25, 27-34, and 36-46.

## IV. STATUS OF AMENDMENTS

No amendments to the claims have been made since the final Office Action, which Action is the subject of this Appeal. A copy of the pending claims is attached to this Brief as Appendix A.

## V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed invention relates to various methods for scanning network devices upon detecting their connection to a network. More specifically, each of the independent claims (1, 15, and 21) recites scanning a first network device "in response to detection of" the first network device. Each independent claim also recites that the scanning is "remote agentless scanning" which "avoid[s] downloading a software agent to the first network device."

### *A. Claims 1 and 15*

Claims 1 and 15 recite a "method for scanning network devices connected to a network" and an "apparatus for remote agentless scanning of network devices," respectively. Claim 1 comprises the following features:

> (a) detecting connection of a first network device to the network;
> (b) performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings there from, the remote agentless scanning being performed automatically in response to detection of the first network device to thereby avoid downloading a software agent to the first network device;
> (c) comparing the internal security settings determined through the remote agentless scanning with predefined security settings to determine compliance therewith; and
> (d) automatically performing a remote installation of a security software program on the first network device if the internal security settings are not in compliance with the predefined network settings.

Claim 15 recites similar features for an apparatus claim. The following discussion provides a concise explanation of the features of claims 1 and 15. While the following refers to specific line and pages numbers in the specification and specific reference characters in the drawings, embodiments of the following features may be discussed and shown in various other locations in the specification and drawings. Furthermore, as noted in the specification, "it is not intended that [the details in the specification] should be regarded as limitations upon the scope of the invention." *Page 20, lines 15-16.*

*1. Detecting Connection of a First Network Device to the Network*

Claims 1 and 15 recite detecting "connection of a first network device to the network." An embodiment of "detecting connection of a first network device to the network" is shown in at least step 410 of FIG. 4. Detecting connection of a first network device to the network is discussed in the specification in at least the following locations: page 3, line 15 through page 4 line 2; page 9, lines 1-4; page 10, lines 6-8, page 10, line 10 through page 11, line 9; and page 17, line 5 through page 18, line 2.

*2. Performing Remote Agentless Scanning*

Claims 1 and 15 recite performing "remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings there from, the remote agentless scanning being performed automatically in response to detection of the first network device to thereby avoid downloading a software agent to the first network device." An embodiment of remote agentless scanning is shown in at least step 480 of FIG. 4. Step 480 states, "Remotely scan the first network device in response to its detection." Remote agentless scanning is scanning performed "without the use of software loaded on the first network device." *Page 9, lines*

*8-9*. Remote agentless scanning is also discussed in the specification in at least the following locations: page 4, lines 3-15; page 5, lines 6-7; page 5, lines 9-14; page 6, lines 2-3; page 9, lines 4-16; page 10, lines 8-9; page 11, line 7 through page 14, line 5; and page 18, line 2 through page 19, line 20.

3. *Comparing Internal Security Settings with Predefined Security Settings*

Claims 1 and 15 recite "comparing the internal security settings determined through the remote agentless scanning with predefined security settings to determine compliance therewith." An embodiment of this feature of claims 1 and 15 is shown in at least the audit step (step 315) of FIG. 3. The comparing feature is also discussed in the specification in at least the following locations: page 5, lines 16-19; page 11, line 11 through page 12, line 4; page 12, line 18 through page 13, line 4; page 14, line 22 through page 16, line 3; and page 19, lines 13-15.

4. *Automatically Installing a Security Software Program*

Claims 1 and 15 recite "automatically performing a remote installation of a security software program on the first network device if the internal security settings are not in compliance with the predefined network settings." An embodiment of this feature of claim 1 is shown in the compliance step (step 320) of FIG. 3. The installing feature is also discussed in the specification in at least the following locations: page 12, lines 5-17; and page 15 line 22 through page 16, line 3.

***B. Claim 21***

Claim 21 recites a "method for examining a first network device connected to a network." Claim 21 comprises the following features:

(a) querying a database for data representing connection of network devices to a network;

(b) determining connection of a first network device to the network by locating data about the first network device in the database;

(c) determining properties associated with the first network device to determine the identity of the first network device;

(d) determining items to scan based on at least one of the properties; and

(e) performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings there from, the remote agentless scanning being performed automatically in response to the determination of the connection of the first network device to the network to thereby avoid downloading a software agent to the first network device.

The following discussion provides a concise explanation of the features of claim 21. While the following refers to specific line and pages numbers in the specification and specific reference characters in the drawings, embodiments of the following features may be discussed and shown in various other locations in the specification and drawings. Furthermore, as noted in the specification, "it is not intended that [the details in the specification] should be regarded as limitations upon the scope of the invention." *Page 20, lines 15-16.*

*1. Querying a Database*

Claim 21 recites "querying a database for data representing connection of network devices to a network." An embodiment of querying a database is shown in at least step 440 of FIG. 4. Querying a database is discussed in the specification in at least the following locations: page 3, lines 15-21; page 10, line 10 through page 11, line 6; and page 17, line 17 through page 18, line 2.

*2. Determining Connection of a First Network Device*

Claim 21 recites "determining connection of a first network device to the network by locating data about the first network device in the database." An embodiment of determining connection of a first network device is shown in at least step 410 of FIG. 4. Determining connection of a first network device to a network by locating data about the first network device in a

database is discussed in the specification in at least the following locations: page 10, line 10 through page 11, line 6; and page 17, line 17 through page 18, line 2.

*3. Determining Properties Associated with a First Network Device to Determine its Identity*

Claim 21 recites "determining properties associated with the first network device to determine the identity of the first network device." An embodiment of determining properties of a first network device is shown in at least step 445 of FIG. 4. Determining properties of a first network device is discussed in the specification in at least the following locations: page 10, line 10 through page 11, line 6; and page 17, line 17 through page 19, line 5.

*4. Determining Items to Scan Based on At Least One of the Properties*

Claim 21 recites "determining items to scan based on at least one of the properties." An embodiment of determining items to scan is shown in at least step 455 of FIG. 4. Determining items to scan based on at least one of the properties is discussed in the specification in at least the following locations: page 14, line 22 through page 15, line 16; and page 19, lines 6-11.

*5. Performing Remote Agentless Scanning*

Claim 21 recites "performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings therefrom, the remote agentless scanning being performed automatically in response to detection of the first network device to thereby avoid downloading a software agent to the first network device." An embodiment of remote agentless scanning is shown in at least step 480 of FIG. 4. Remote agentless scanning is also discussed in the specification in at least the following locations: page 4, lines 3-15; page 5, lines 6-7; page 5, lines 9-14; page 6, lines 2-3; page 9, lines 4-16; page 10, lines 8-9; page 11, line 7 through page 14, line 5; and page 18, line 2 through page 19, line 20.

## VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-4, 6-10, 12, 14-18, 20-24, 31, 36, and 44 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application No. 2003/0212779 to Boyter et al. ("Boyter") in view of U.S. Patent Application No. 2005/0050335 to Liang et al. ("Liang"). Claims 38 and 41 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in View of Liang, and further in view of U.S. Patent Application No. 2005/0015760 to Ivanov et al. ("Ivanov"). Claims 27-30 and 33-34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in view of Liang, and further in view of U.S. Patent No. 6,993,448 to Tracy et al ("Tracy").

Claim 5 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in view of Liang, and further in view of U.S. Patent Application No. 2001/0047401 to Moore et al. ("Moore"). Claims 13, 19, and 25 stand rejected under 35 U.S.C. § 103(a) to Boyter in view of Liang, and further in view of U.S. Patent Application No. 2004/0268145 to Watkins et al. ("Watkins"). Claims 32 and 37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in view of Liang, and further in view of U.S. Patent No. 6,546,493 to Medic et al. ("Medic"). Claims 39, 42, and 45 stand rejected under 35 U.S.C. § 103 (a) as being unpatentable over Boyter in view of Liang. Claims 40, 43, and 46 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in view of Liang, and further in view of U.S. Patent Application No. 2006/0010492 to Heintz et al. ("Heintz").

Appellants respectfully request that these grounds of rejection be reviewed in the instant Appeal.

## VII. ARGUMENT

### *A. The Examiner has not Established a Prima Facie Case of Obviousness with Respect to Claims 1, 3, 4, 6-10, 12, 14-18, 20-24, 31, 36, and 44 are not*

The Examiner has not established a *prima facie* case of obviousness for the claim rejections based on Boyter in view of Liang because (1) the Examiner has not accurately resolved the Graham factual inquiries and (2) the Examiner has not articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.

*1. The Examiner did not accurately resolve the Graham factual inquiries*

A conclusion of obviousness "must be resolved on the basis of [the *Graham*] factual determinations." *MPEP 2141*. These factual determinations include "ascertaining the differences between the claimed invention and the prior art." *Id.* Both Boyter and Liang fail to show, teach, or suggest "remote agentless scanning being performed automatically *in response to* detection of the first network device," as recited in element (b) of claim 1. *Emphasis added.* The Examiner notes that Boyter "fails to teach . . . the remote agentless scanning being performed automatically in response to detection of the first network device." *Final Office Action, Page 4*. However, the Examiner asserts that Liang, in paragraphs 0093-0097, teaches this feature of claim 1. *Final Office Action, Pages 4-5*. Appellants disagree.

An important difference between Liang and claim 1 is that Liang does not teach or suggest the claimed relationship between remote agentless scanning and detection of a network device (*i.e.*, performing remote agentless scanning in response to the detection of a network device). In fact, Liang does not even teach remote agentless scanning. Instead, Liang merely teaches that "a determination is made whether or not a proper set of anti-virus policies and protocols are in place

[on a new client device that is permanently added to the network]." *Paragraph 0095*. However, even if Liang's determination could be compared to remote agentless scanning (Appellants show below why Liang does not teach remote agentless scanning), Liang would still fail to teach the features of element (b) of claim 1 because Liang does not teach that the determination is performed in response to detecting a connection of the new client device. Indeed, Liang does not address detecting the connection of the new client device to the network.

Liang's failure to address "remote agentless scanning being performed automatically in response to detection of the first network device" may be related to Liang's failure to recognize the problems addressed by claim 1. By performing remote agentless scanning on a network device in response to detection of the network device, claim 1 addresses the problems that arise "with computers that ordinarily connect to the network using transient means, such as a virtual private network connection or using a wireless access point." *Specification, pages 2-3*. In such situations, if the scanning is not performed in response to the connection of the network device, "the device may not be available at the time that the scan occurs because of the transient nature of the connection." *Id.* For example, if a laptop temporarily connects to a wireless network, the laptop may disconnect from the network before the laptop is scanned.

Similarly, when scanning is not performed in response to the connection of the network device, there may be "a significant delay between the time that a device attaches, or connects, to the network and the time that the scan occurs . . . [and this] time lag may result in a network being infected before a scan has occurred." *Id.* Liang does not address these problems and consequently does not provide the solution recited in claim 1.

In addition to failing to teach "scanning being performed automatically in response to detection of the first network device," Liang and Boyter also both fail to teach "performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings therefrom," as recited in claim 1. The Examiner notes that "Boyter et al. fails to perform remote agentless scanning of internal files and data within the internal files on the first network device," and the Examiner suggests that Liang, in paragraphs 0093-0097, remedies this deficiency of Boyter. *Final Office Action, pages 4-5.* Appellants disagree.

Liang does not determine internal security settings of a network device by performing remote agentless scanning. Liang teaches that "a determination is made whether or not a proper set of anti-virus policies and protocols are in place" on a client device, but does not teach that the determination is made through remote agentless scanning. *Paragraph 0095.* Instead, Liang suggests an interactive process for determining whether the appropriate anti-virus software is installed on client devices. For example, Liang teaches that a "virus monitor 102 will perform an anti-virus security policy procedure whereby each of the client devices coupled to virus monitor 102 is queried in order to determine if that client device has the appropriate and proper anti-virus software installed," and "upon receiving the query 140, each of the client devices checks for confirmation that the appropriate anti-virus software is indeed present." *Paragraphs 0053-0055.*

Liang's procedure for determining whether a client device has the appropriate and proper anti-virus software installed is not comparable to remote agentless scanning. In Liang, the client device itself checks for confirmation that the appropriate anti-virus software is present. Liang's self-check process is performed through local confirmation, not remote scanning. Indeed, remote agentless scanning is performed "without the use of software loaded" on the network device.

*Paragraph 0030.* In contrast, Liang's process appears to utilize software on the client device to check for anti-virus software. Thus, with respect to determining internal security settings, Liang fails to teach remote agentless scanning and instead teaches a process quite different from remote agentless scanning. Accordingly, both Liang and Boyter fail to teach "performing remote agentless scanning to determine internal security settings," as recited in claim 1.

The Examiner's response to Appellant's point that Liang does not teach "remote agentless scanning" is that "Liang clearly teaches wherein Specifically, in a particular embodiment of the invention, when a visitor connects a heretofore unknown (to network) client device as shown in FIG. 3, virus monitor will query the visitor client device for the presence of appropriate anti-virus software." *Final Office Action, page 2.* However, the Examiner's response does not address the problem that in Liang, "upon receiving the query 140, each of the client devices checks for confirmation that the appropriate anti-virus software is indeed present." *Paragraphs 0053-0055.* In other words, Liang suggests that scanning is performed by the client itself, which is not remote agentless scanning, and the Examiner does not address this deficiency of Liang.

As shown, neither Boyter nor Liang discloses "remote agentless scanning being performed automatically in response to detection of the first network device," as recited in element (b) of claim 1. Furthermore, neither Boyter nor Liang discloses "performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings therefrom." Accordingly, any determination of obviousness must be resolved in view of these differences between claim 1 and the cited references. The Examiner fails to acknowledge these distinctions and therefore does not provide a proper basis for a determination of

obviousness. The rejection of claim 1 under 35 U.S.C. § 103(a) is therefore improper and Appellants respectfully request reversal of the same.

*2. The Examiner has not articulated reasoning with some rational underpinning to support the legal conclusion of obviousness*

The Federal Circuit held, and the Supreme Court confirmed, that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). See also *KSR Int'l Co. v. Teleflex,* 550 U.S. at ___ , 82 USPQ2d at 1396 (2007) (quoting Federal Circuit statement with approval). The Examiner appears to base the finding of obviousness on the reasoning that "some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to combine prior art reference teachings to arrive at the claimed invention," but does not satisfy the requirements of establishing a case of *prima facie* obviousness based on this rationale. *MPEP 2143*. According to section 2143 of the MPEP:

> To reject a claim based on this rationale . . . Office personnel must articulate the following: (1) a finding that there was some teaching, suggestion, or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.

The teaching from Liang cited by the Examiner does not provide any suggestion or motivation for combining Liang with Boyter to provide the features of claim 1.

The Examiner's reasoning for combining Boyter and Liang is a quote from the background of Liang about the problems addressed by Liang, but is not related to the problems addressed (or the solutions provided) by claim 1. According to the Examiner,

> It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Liang et al in the claimed

> invention of Boyter et al in order to provide an anti-virus method and system having multilevel anti-virus function for anticipating and detecting computer virus outbreak (See page 2, paragraph [0013]).

*Page 4.* The Examiner's reasoning does not show why a skilled artisan would have found the claimed invention obvious in light of the teachings of Boyter and Liang. Indeed, even if the Examiner's reasoning is correct and a combination of Boyter and Liang provides a system with "multilevel anti-virus function for anticipating and detecting computer virus outbreak," such a combination does not provide remote agentless scanning performed in response to detection of a network device.

As shown, the Examiner has not established a *prima facie* case of obviousness because the Examiner has not accurately resolved the Graham factual inquiries or provided adequate reasoning to support the legal conclusion of obviousness. Claim 1 is allowable over Boyter and Liang for at least this reason. These arguments apply with equal force to independent claims 15 and 21. Thus, independent claims 1, 15, and 21, as well as claims 3, 4, 6-10, 12, 14, 16-18, 20, 22-24, 31, 36, and 44, which depend from claims 1, 15, and 21, are allowable over Boyter in view of Liang. Appellants therefore request reversal of the rejections of claims 1, 3, 4, 6-10, 12, 14, 15, 16-18, 20, 21, 22-24, 31, 36, and 44.

### *B. Neither Boyter Nor Liang Teaches Inspecting Data Packets Communicated Over the Network, as Recited in Claim 2*

Claim 2 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in view of Liang. Claim 2 depends from claim 1 and is allowable for at least the same reasons that claim 1 is allowable. Claim 2 also distinguishes over the cited references for various other reasons.

Both Boyter and Liang fail to teach the features recited in claim 2. Claim 2 recites that detecting connection of a first network device to the network further comprises "inspecting data packets communicated over the network." The Examiner asserts that Boyter, in paragraph 0012, teaches this feature. *Final Office Action, page 5.* In paragraph 0012, Boyter states "scanning all network host nodes within designated address ranges for determining all active hosts," but Applicants are unable to find any teaching of inspecting data packets to detect connection of a network device.

Instead of teaching the features of claim 2, Boyter teaches a scanning technique that appears to suffer from problems identified in the background of the present application. Boyter "performs a discovery scan against all potential hosts within [a] defined range . . . on a frequent basis, allowing for a more rapid detection of new or removed hosts." *Paragraph 0021.* Despite Boyter's focus on rapid detection of new hosts, Boyter's process suffers from numerous deficiencies. For example Boyter only performs the scan within designated address ranges and may not detect any devices outside the designated ranges. *Paragraph 0012.* Furthermore, Boyter's scan appears to be a periodic scanning technique that suffers from numerous drawbacks.

The background of the present application notes that there are "numerous drawbacks associated with [periodic scanning]." *Page 2.* For example:

> One drawback is that the scan may not be comprehensive because some devices may have, for some reason, been turned off at the time of the scan and, consequently, may not have been scanned. Another shortcoming with periodic scanning is that there may be a significant delay between the time that a device attaches, or connects, to the network and the time that the scan occurs during the next scheduled scan. This time lag may result in a network being infected before a scan has occurred. . . . A third weakness is that the periodic scan does not work well with computers that ordinarily connect to the network using transient means, such as with a virtual private network connection or using a wireless access point. In particular, the device may not be

> available at the time that the scan occurs because of the transient nature of the connection.

*Pages 2-3.* Boyter does not address these issues. In contrast, claim 2 provides an event-driven (rather than periodic) network-device detection process. As recited in claim 2, network devices are detected by "inspecting data packets communicated over the network," which addresses the drawbacks identified in the background and distinguishes over Boyter. For at least this reason, claim 2 further distinguishes over Boyter and Liang. The rejection of claim 22 under 35 U.S.C. § 103(a) is therefore improper and Appellants respectfully request reversal of the same.

### *C. Claims 38 and 41 are patentable over Boyter in view of Liang and Ivanov*

Claim 38 and 41 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in view of Liang, and in further view of U.S. Patent Application No. 2005/0015760 to Ivanov et at. ("Ivanov"). Claims 38 and 41 depend from claims 1 and 15 and are allowable for at least the same reasons that claims 1 and 15 are allowable. The rejections of claims 38 and 41 under 35 U.S.C. § 103(a) are therefore improper and Appellants respectfully request reversal of the same.

### *D. Claims 27-30 and 33-34 are patentable over Boyter in view of Liang and Tracy*

Claims 27-30 and 33-34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in view of Liang and in further view of U.S. Patent No. 6,993,448 to Tracy et al. ("Tracy"). Claims 27-30 and 33-34 depend from claims 1 and 15 and are allowable for at least the same reasons that claims 1 and 15 are allowable. The rejections of claim 27-30 and 33-34 under 35 U.S.C. § 103(a) are therefore improper and Appellants respectfully request reversal of the same.

***E. Claim 5 is Patentable over Boyter in view of Liang and Moore***

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Boyter in view of Liang and in further view of U.S. Patent Application No. 2001/0047401 to Moore et al. ("Moore"). Claim 5 depends from claim 1 and is allowable for at least the same reasons that claim 1 is allowable. The rejection of claim 5 under 35 U.S.C. § 103(a) is therefore improper and Appellants respectfully request reversal of the same.

***F. Claims 13, 19, and 25 are patentable over Boyter in view of Liang and Watkins***

Claims 13, 19, and 25 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in view of Liang and further in view of U.S. Patent Application No. 20040268145to Watkins et al. ("Watkins"). Claims 13, 19, and 25 depend from claims 1, 15, and 21 and are allowable for at least the same reasons that claims 1, 15, and 21 are allowable. The rejections of claims 13, 19, and 25 under 35 U.S.C. § 103(a) are therefore improper and Appellants respectfully request reversal of the same.

***G. Claims 32 and 37 are patentable over Boyter in view of Liang and Magdych***

Claims 32 and 37 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Boyter in view of Liang and further in view of U.S. Patent No. 6,6546,49 to Magdych et al ("Magdych"). Claims 32 and 37 depend from claims 1 and 15 and are allowable for at least the same reasons that claims 1 and 15 are allowable. The rejections of claims 32 and 37 under 35 U.S.C. § 103(a) are therefore improper and Appellants respectfully request reversal of the same.

***H. Claims 39, 42, and 45 are patentable over Boyter in view of Liang***

Claims 39, 42, and 45 are rejected under 35 U.S.C S 103(a) as being unpatentable over Boyter in view of Liang. Claims 39, 42, and 45 depend from claims 1, 15, and 21 and are allowable for at least the same reasons that claims 1, 15, and 21 are allowable. The rejections of claims 39, 42, and 45 under 35 U.S.C. § 103(a) are therefore improper and Appellants respectfully request reversal of the same.

***Claims 40, 43, and 46 are Patentable over Boyter in view of Liang and Heintz***

Claims 40, 43, and 46 stand rejected under 35 U.S.C.§ 103(a) as being unpatentable over Boyter in view of Liang and in further view of U.S. Patent Application No. 2006/0010492 to Heintz et al ("Heintz"). Claims 40, 43, and 46 depend from claims 1, 15, and 21 and are allowable for at least the same reasons that claims 1, 15, and 21 are allowable. The rejections of claims 40, 43, and 46 under 35 U.S.C. § 103(a) are therefore improper and Appellants respectfully request reversal of the same.

## VIII. CLAIMS APPENDIX

A copy of the claims involved in the present appeal is attached hereto as Appendix A. As indicated above, the claims in Appendix A represent the state of the claims as pending.

## IX. EVIDENCE APPENDIX

No evidence pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or entered by the Examiner is being submitted.

## X. RELATED PROCEEDINGS APPENDIX

As detailed in Section II above, Appellants are not aware of any other appeals, interferences, or judicial proceedings that will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

## XI. CONCLUSION

For at least the foregoing reasons, Appellants believe that each of the finally rejected claims in this application is in immediate condition for allowance. Accordingly, Appellants respectfully request the reversal of the rejections of these claims and allowance of the same.

Respectfully submitted,

Date: 23 July 2008

Bryan K. Hanks
Registration No. 52,991

Enclosures: Transmittal of Appeal Brief
Appendix A: Claims

## APPENDIX A

**Claims Involved in the Appeal of Application No. 10/683,564**

1. (previously presented) A method for scanning network devices connected to a network, comprising:

(a) detecting connection of a first network device to the network;

(b) performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings there from, the remote agentless scanning being performed automatically in response to detection of the first network device to thereby avoid downloading a software agent to the first network device;

(c) comparing the internal security settings determined through the remote agentless scanning with predefined security settings to determine compliance therewith; and

(d) automatically performing a remote installation of a security software program on the first network device if the internal security settings are not in compliance with the predefined network settings.

2. (original) The method of claim 1 wherein step (a) further comprises inspecting data packets communicated over the network.

3. (original) The method of claim 1 wherein the detecting step further comprises querying a database.

4. (original) The method of claim 3 further comprising continuously broadcasting pings on the network, continuously examining address resolution protocol tables, continuously monitoring event logs, transmitting a Lightweight Directory Access Protocol (LDAP) query, and transmitting a Domain Name System query.

5. (original) The method of claim 1 wherein step (b) further comprises determining at least one of whether the first network device is plugged into a wall socket, whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via a Virtual Private Network.

6. (original) The method of claim 1 wherein step (b) further comprises determining a property of the first network device.

7. (previously presented) The method of claim 1 wherein step (b) further comprises determining an identity of the first network device.

8. (original) The method of claim 7 wherein the determining of the identity of the first network device further comprises at least one of querying a database where the type has been determined, examining network traffic, analyzing network behavior, probing the first network device for signature responses, attempting to log into the device using a series of protocols, logging into the first network device and querying data within the device.

9. (original) The method of claim 1 wherein step (b) further comprises scanning at least one of a configuration, file, data, a software version, a patch, inventory, hardware, and a security vulnerability of the first network device.

10. (original) The method of claim 1 wherein step (b) further comprises updating at least one of a configuration, file, data, a software version, inventory, and a security vulnerability of the first network device.

11. (canceled)

12. (previously presented) The method of claim 1 wherein step (b) further comprises determining if the first network device is part of a windows domain.

13. (original) The method of claim 1 further comprising at least one of enabling the first network device to have additional access to the network, denying the first network device access to the network, notifying another about the first network device based on results of the scan, and quarantining the first network device.

14. (original) The method of claim 1 further comprising at least one of setting a security policy on the first network device, auditing the security policy of the first network device, ensuring compliance with a predetermined security policy, and reporting results.

15. (previously presented) An apparatus for remote agentless scanning of network devices on a network comprising:

(a) a detecting module that detects connection of a first network device to the network; and

(b) a scanning module that performs remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings there from, the remote agentless scanning being performed automatically in response to the detection of the first network device to thereby avoid downloading a software agent to the first network device;

(c) comparing the internal security settings determined through the remote agentless scanning with predefined security settings to determine compliance therewith; and

(d) automatically performing a remote installation of a security software program on the first network device if the internal security settings are not in compliance with the predefined network settings.

16. (original) The apparatus of claim 15 wherein the detecting module continuously polls a database for data corresponding to newly attached network devices

17. (original) The apparatus of claim 16 wherein the scanning module remotely scans the first network device upon detecting data corresponding to the first network device in the database.

18. (original) The apparatus of claim 15further comprising a history database storing scan results of a scan performed by the scanning module.

19. (original) The apparatus of claim 15 wherein the scanning module can at least one of enable the first network device to have additional access to the network, deny the first network device access from the network, notify another about the first network device based on results of the scan, and quarantine the first network device.

20. (original) The apparatus of claim 15 further comprising a security policy management module for at least one of setting a security policy on the first network device, auditing the security policy of the first network device, ensuring compliance with a predetermined security policy, and reporting results.

21. (previously presented) A method for examining a first network device connected to a network, comprising:

(a) querying a database for data representing connection of network devices to a network;

(b) determining connection of a first network device to the network by locating data about the first network device in the database;

(c) determining properties associated with the first network device to determine the identity of the first network device;

(d) determining items to scan based on at least one of the properties; and

(e) performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings there from, the remote agentless scanning being performed automatically in response to the determination of the connection of the first network device to the network to thereby avoid downloading a software agent to the first network device.

22. (original) The method of claim 21 wherein step (c) further comprises determining at least one of credentials associated with the first network device and type of the first network device.

23. (original) The method of claim 21 wherein step (c) further comprises at least one of querying a database where the identity has already been determined, examining network traffic, analyzing network behavior, probing the device for signature responses, and logging into the device to query data.

24. (original) The method of claim 21 wherein step (e) further comprises selecting a set of security policy settings to audit.

25. (original) The method of claim 21 further comprising at least one of allowing the first network device to have additional access to the network, denying access to the network, notifying another about the first network device based on results of the remote scanning, and quarantining the first network device.

26. (canceled)

27. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning a stored configuration of hardware and software on the first network device.

28. (previously presented) The method of claim 27 wherein the scanning of internal files and data in step (b) comprises scanning for incorrectly configured hardware and software.

29. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning for incorrectly configured hardware and software.

30. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning to determine a software version.

31. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning a software patch.

32. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning for viruses.

33. (previously presented) The apparatus of claim 15 wherein the scanning module scans a configuration of hardware and software on the first network device.

34. (previously presented) The method of claim 15 wherein the scanning module scans to determine a software version.

35. (canceled)

36. (previously presented) The method of claim 15 wherein the scanning module scans a software patch.

37. (previously presented) The apparatus of claim 15 wherein the scanning module scans for viruses.

38. (previously presented) The method of claim 31 wherein automatically performing a remote installation of a security software program in step (d) comprises installing a new version of the software patch.

39. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises searching for a predetermined anti-virus software, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the predetermined anti-virus software if the predetermined anti-virus software is not found in step (b).

40. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises determining whether firewall software is installed, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the firewall software if it is determined in step (b) that the firewall software has not yet been installed.

41. (previously presented) The method of claim 36 wherein automatically performing a remote installation of a security software program in step (d) comprises installing a new version of the software patch.

42. (previously presented) The method of claim 15 wherein the scanning of internal files and data in step (b) comprises searching for a predetermined anti-virus software, and wherein

automatically performing a remote installation of a security software program in step (d) comprises installing the predetermined anti-virus software if the predetermined anti-virus software is not found in step (b).

43. (previously presented) The method of claim 15 wherein the scanning of internal files and data in step (b) comprises determining whether firewall software is installed, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the firewall software if it is determined in step (b) that the firewall software has not yet been installed.

44. (previously presented) The method of claim 21 further comprising comparing the internal security settings determined through the remote agentless scanning of internal files and data with predefined security settings to determine compliance therewith.

45. (previously presented) The method of claim 21, wherein the remote agentless scanning comprises searching the first network device to determine whether anti-virus software is installed on the first network device.

46. (previously presented) The method of claim 21, wherein the remote agentless scanning comprises searching the first network device to determine whether firewall software is installed on the first network device.